Malware 101

Introduction to ransomware and how to protect your organization against these emerging threats

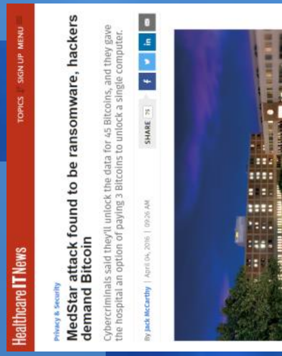
UCCSC 2016

July 11th 2016

David Lam
IT Security
UC Davis Medical Center
davlam@ucdavis.edu

Why should we care?

- Hospitals are easy targets for attackers.
  - Many hospitals are already in the headlines for its association with ransomware: Hollywood Presbyterian, Kansas Heart, MedStar Health.
- Ransomware can bring down critical assets and systems.
- Ransomware is a business – Criminals collected over $209 million in the first three months of 2016 - FBI

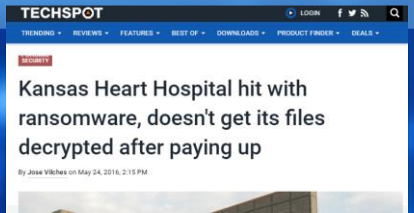


Privacy & Security

MedStar attack found to be ransomware, hackers demand Bitcoin

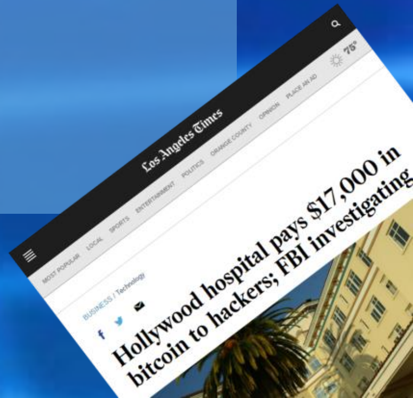
Cybercriminals said they'll unlock the data for 45 Bitcoins, and they gave the hospital an option of paying 3 Bitcoins to unlock a single computer.

By Jack McCarthy | April 04, 2016 | 09:26 AM



Kansas Heart Hospital hit with ransomware, doesn't get its files decrypted after paying up

By Jose Vilches on May 24, 2016, 2:15 PM



Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

What is Ransomware?

ran·som·ware

ˈransəmˌwe(ə)r/

noun

- a type of malicious software designed to block access to a computer system until a sum of money is paid.

- Google

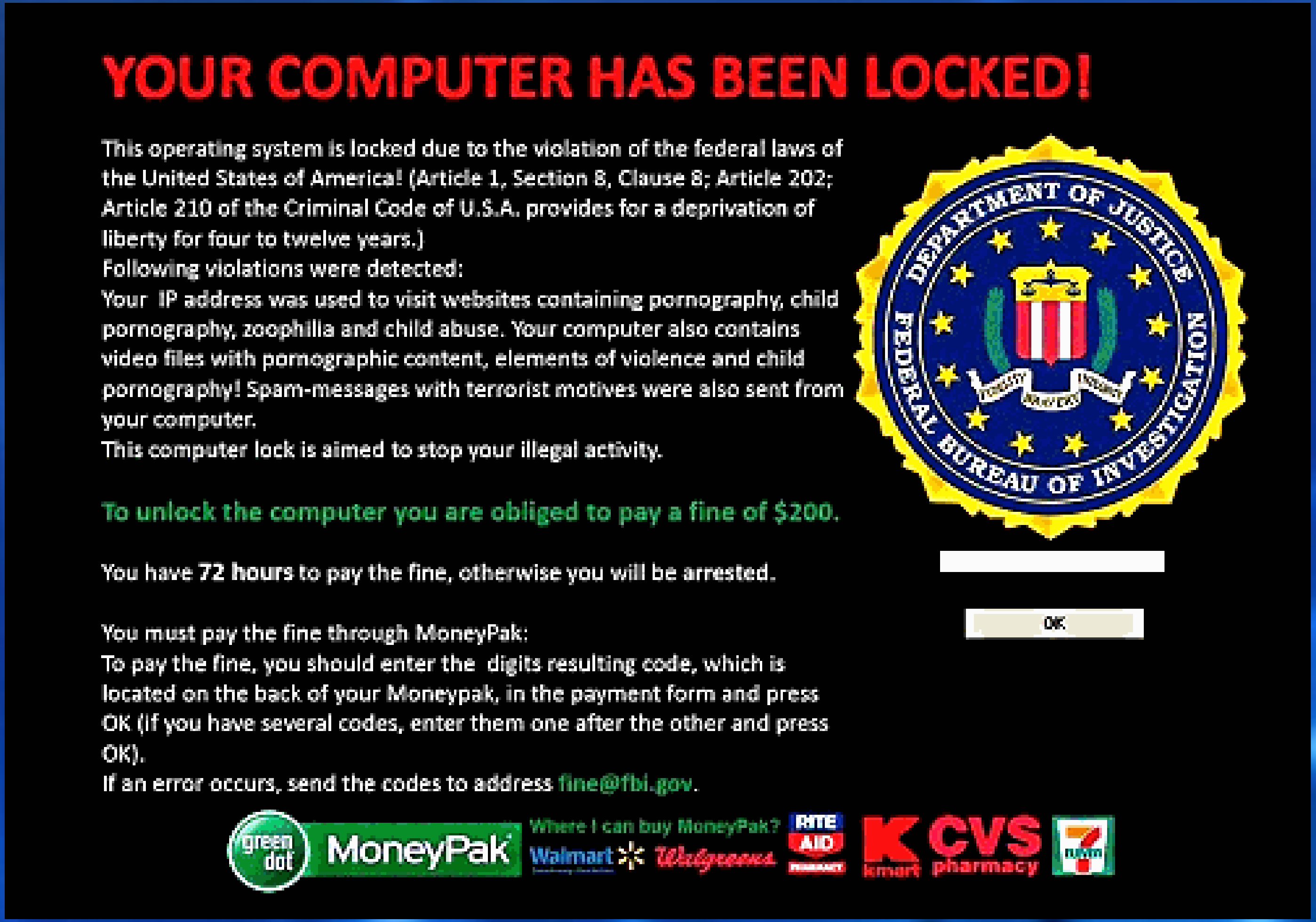
Types of Ransomware

- Non-Encrypting Ransomware / Trojans / Hoaxes
- Encrypting Ransomware (common ransomware)
- Web-based Ransomware

Non-Encrypting Ransomware / Trojans / Hoaxes

- Arrives through the user’s inbox, web browser, or other telecommunications means.
- Threatens the user that adverse action would be taken against them or their account(s).
- Does not encrypt files, but demands financial information or a ransom to resolve adverse action.

“Police” Ransomware



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

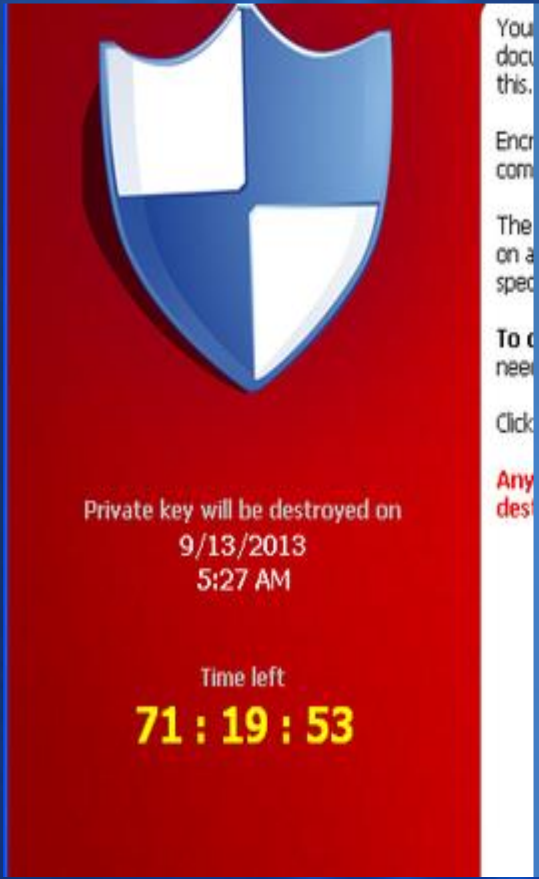
You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Deadly Consequences of Ransomware

Joseph Edwards, 17

- Suffered from Autism
- Received an email from Cheshire police demanding a ransom of £100 or face prosecution due to extreme pornography, breach of copyright, and terrorism.
- Hanged himself in his own home after receiving false email

Encrypting Ransomware (common ransomware)



Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

You
docu
this.

Encr
com

The
on a
spec

To c
nee

Click

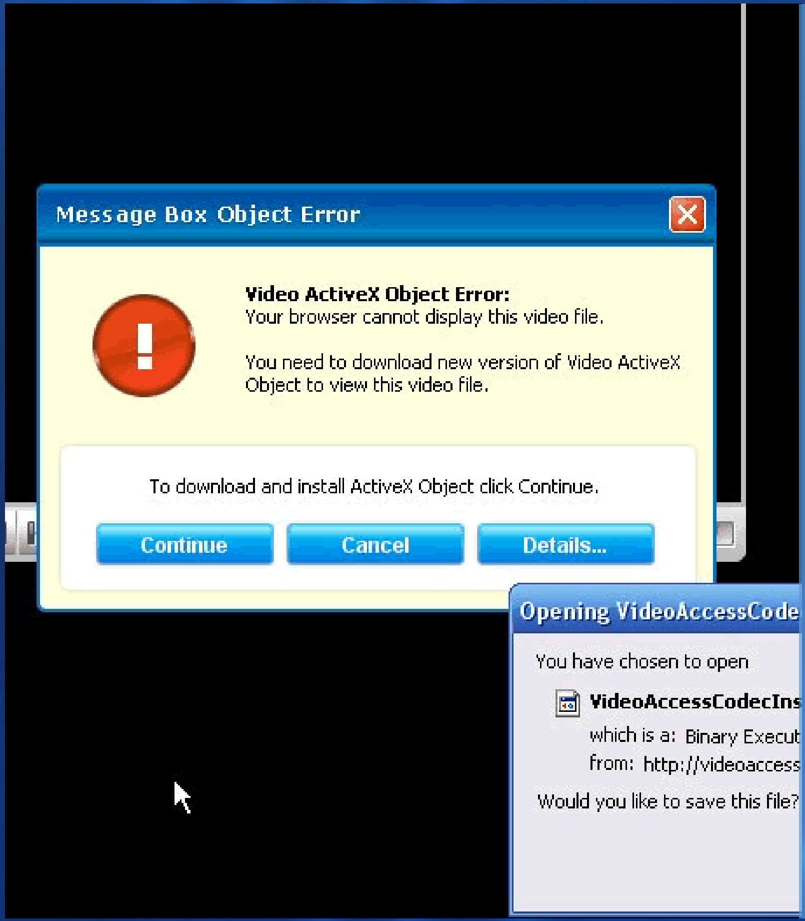
Any
des

- First known ransomware named AIDS – 1989.
- Encrypting ransomware returned back to prominence with the introduction of ***CryptoLocker*** in 2013.
- Many different variants and strains released since that time.
- Many infection vectors, including malvertising, drive-by download , exploit-kits, email, server vulnerabilities, etc.

Malvertising Vector

- Most websites on the Internet use one or more advertising networks to deliver advertising to its visitors.
- Smaller advertising networks may not have proper security in place to thwart targeted attacks.
- Infected ad networks distribute malicious content on well known sites such as CBS or Blogger.

Drive-by Downloads



Message Box Object Error

Video ActiveX Object Error:
Your browser cannot display this video file.

You need to download new version of Video ActiveX Object to view this video file.

To download and install ActiveX Object click Continue.

Opening VideoAccessCode

You have chosen to open

VideoAccessCodecIns

which is a: Binary Execut
from: http://videoaccess

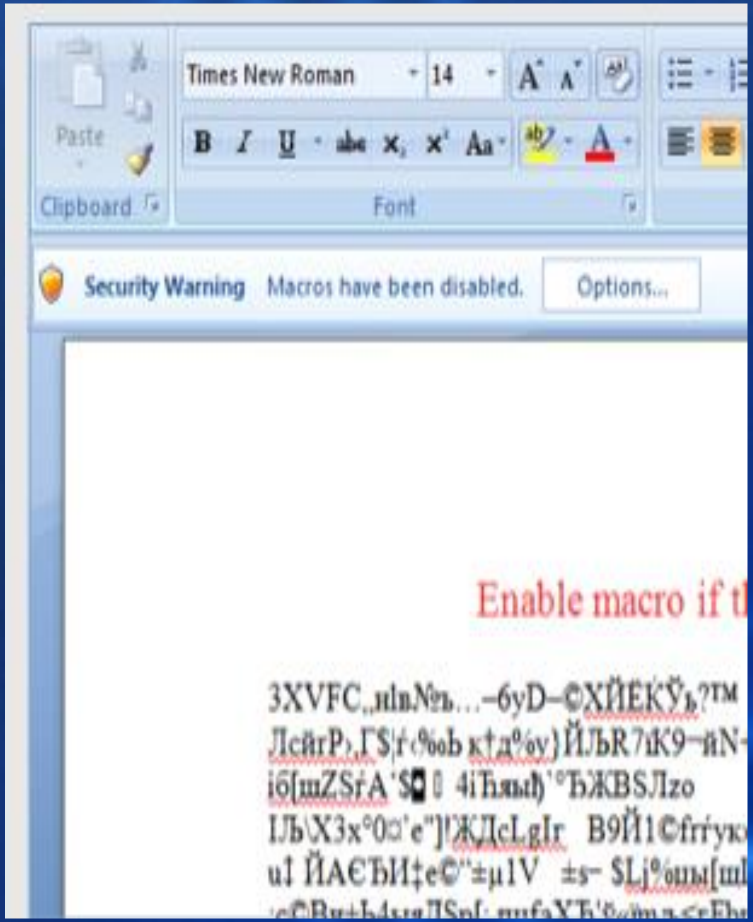
Would you like to save this file?

- Generally advises user that they need an update to their system, or that their system is infected and requires immediate attention.
- Delivers many classes of malware, including ransomware.
- Malvertising threat actors can redirect visitors to malicious downloads on legitimate sites, increasing the chances of successful execution.

Exploit-Kit Vectors

- Highly specialized malware targets browser add-ons and their vulnerabilities.
- Many variants are highly polymorphic and employs sophisticated encryption / obfuscation techniques to evade detection by various security technologies.
- Examples: ***Angler EK, Neutrino EK, RIG EK***.
- Serves as a conduit for malicious software to be installed on the victim’s computer.

Email Vector



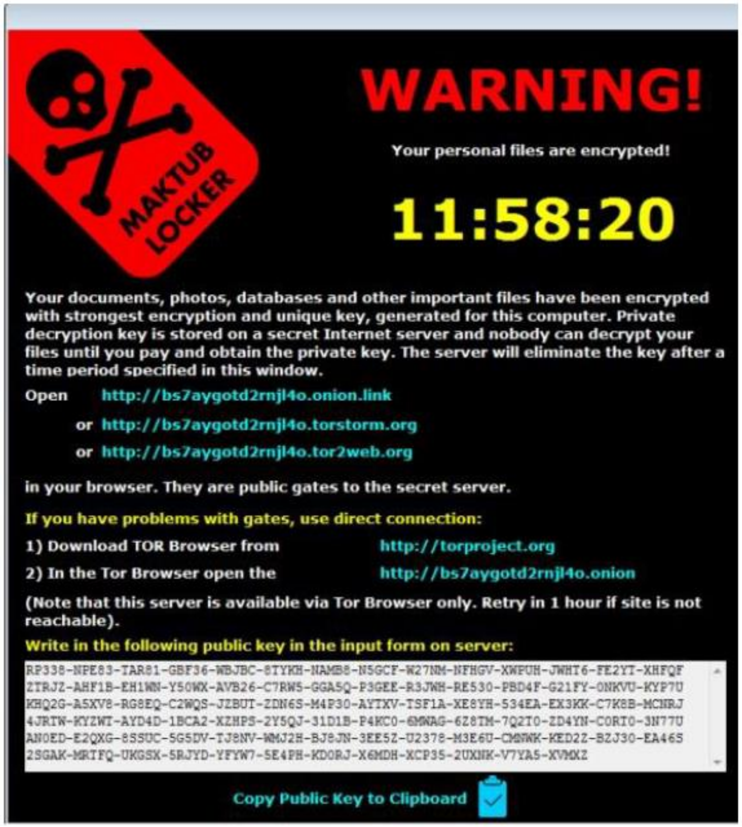
Security Warning Macros have been disabled.

Enable macro if t

```
3XVFC„нlпNoђ…–6yD–©XЙЁKЎ»?™
ЛсйгР›,Г$|ŕ‹‰ь к†д°⁄oу}ЙЉR7iK9¬йN
i6[шZSŕA'$■ ▯ 4iЋяы)'°ЪЖBSЛzo
IЉ\X3x°0¤'e"]!ЖДсLgIr  B9Й1©frŕyк
u↨ ЙАЄЪИ‡е©"±µ1V  ±s– $Lj%ыы[ш
```

- Uses deception in order to get the user to open an attachment or a link inside the email.
- Emails regarding tax forms, voicemails, and pending packages are very common.
- Emails can be targeted to the organization (e.g. healthcare forms, HR related activities, etc)
- Some types of ransomware specializes in email delivery (e.g. ***Locky***)

Server Vulnerabilities Vectors



WARNING!

Your personal files are encrypted!

11:58:20

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://bs7aygotd2rnjl4o.onion.link
or http://bs7aygotd2rnjl4o.torstorm.org
or http://bs7aygotd2rnjl4o.tor2web.org

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1) Download TOR Browser from http://torproject.org

2) In the Tor Browser open the http://bs7aygotd2rnjl4o.onion

(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input form on server:

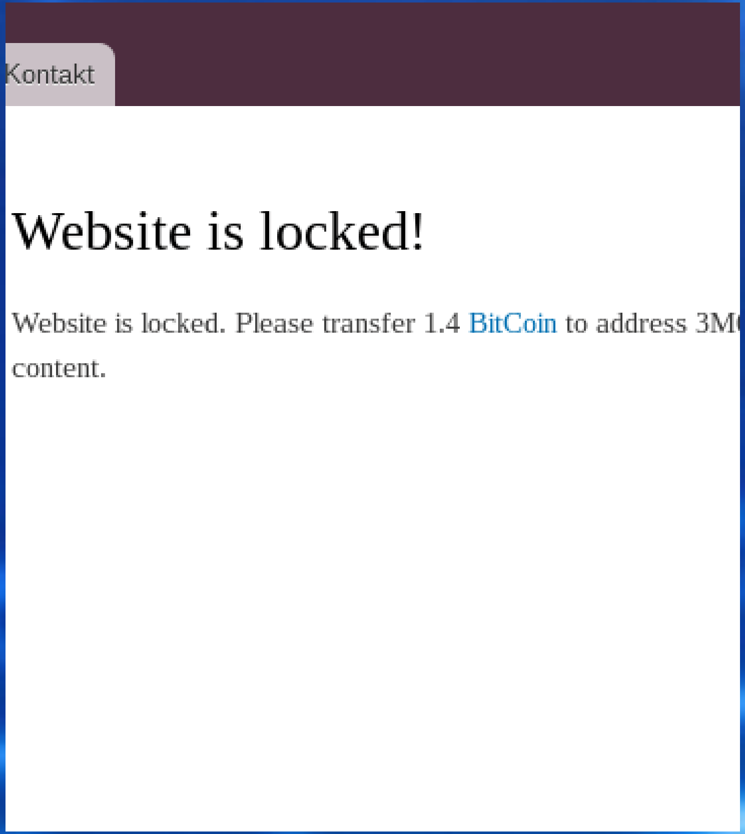
```
RP338-NPE83-TAR81-GBF36-WBJBC-8TYKH-NAMB8-N5GCF-W27NM-NFHGV-XWPUH-JWHT6-FE2YT-XHFQF
ZTRJZ-AHF1B-EH1WN-Y50WX-AVB26-C7RW5-GGA5Q-P3GEE-R3JWH-RE530-PBD4F-G21FY-0NKVU-KYP7U
KHQ2G-A5XV8-RG8EQ-C2WQS-JZBUT-ZDN6S-M4P30-AYTXV-TSF1A-XE8YH-534EA-EX3KK-C7K8B-MCNRJ
4JRTW-KYZWT-AYD4D-1BCA2-XZHPS-2Y5QJ-31D1B-P4KC0-6MWAG-6Z8TM-7Q2T0-ZD4YN-C0RT0-3N77U
AN0ED-E2QXG-8SSUC-5G5DV-TJ8NV-WMJ2H-BJ8JN-3EE5Z-U2378-M3E6U-CMNWK-KED2Z-BZJ30-EA465
2SGAK-MRTFQ-UKGSX-5RJYD-YFYW7-5E4PH-KD0RJ-X6MDH-XCP35-2UXNK-V7YA5-XVMXZ
```

Copy Public Key to Clipboard

- Unlike other user initiated attack vectors, this vector is initiated by the attacker themselves.
- The vulnerable application is exploited over the Internet and ransomware is deployed on the affected servers.
- Infection may spread across the network using stolen credentials (e.g. SamSam).

Web-Based Ransomware

- Targets the website itself rather than the client machine / device.
- Generally targets out of date content management systems such as Drupal or Wordpress.
- Requires payment to unlock the content of the site.
- Less common than exploit-kit variants.

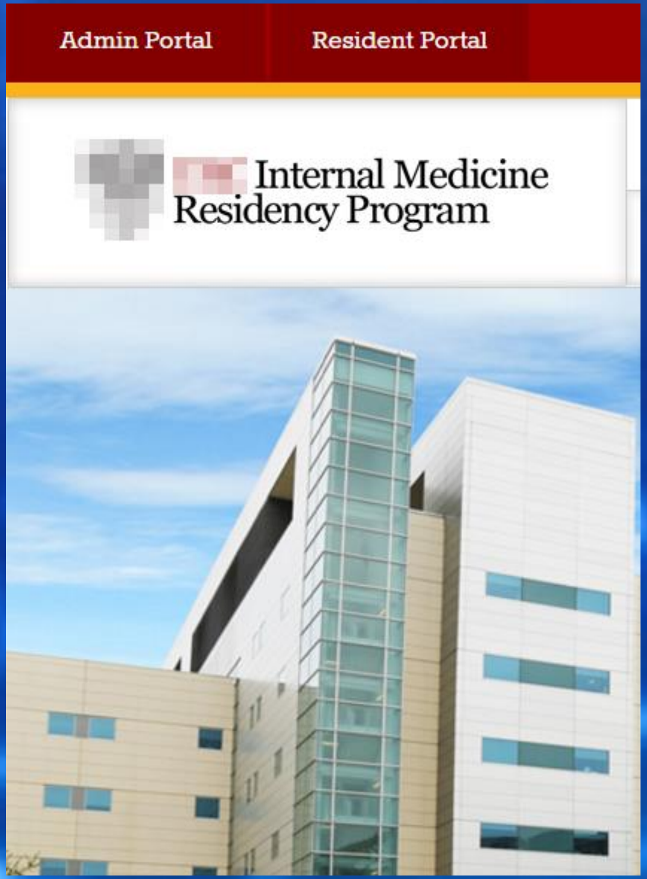


Website is locked!

Website is locked. Please transfer 1.4 BitCoin to address 3M
content.

Web-Based Ransomware (EK Variant)

- No apparent signs of infection on the website.
- Infection can be difficult to locate once infected.
- Redirects visitors to exploit-kit landing pages in the background.
- Frequently occurs on publicly facing CMS sites that are not actively managed and updated.



[redacted] Internal Medicine Residency Program

What should we do?

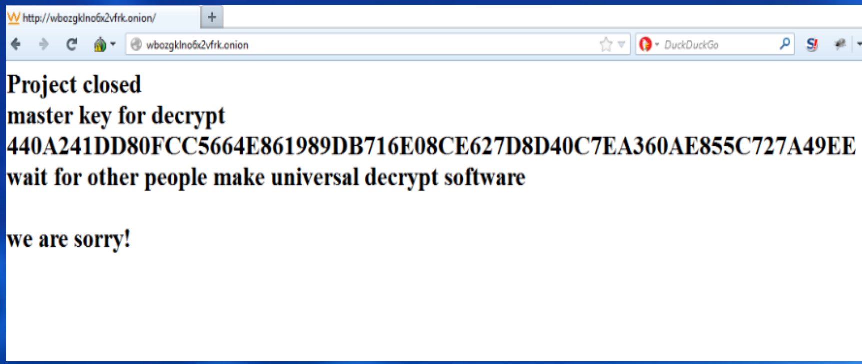
Pay the Ransom?

- My answer: Never pay the ransom!
- Encourages the creation of more sophisticated variants and targeted attacks.
- Paying the ransomware does not guarantee decryption, as Kansas Heart Hospital has experienced.
  - You may become a repeat target for paying the ransom.
- Prevention is key!

Backups, backups, backups!

- Should be part of the business continuity plan (BCP).
- Do backups right!
  - Make sure all critical data is backed up and tested.
  - Backup targets shall not be directly accessible to the device (i.e. offline / air-gapped).
  - Versioning is important to prevent encrypted files from overwriting originals.
- Backup encrypted files before restoration if backups are not available.

All your important files are encrypted.

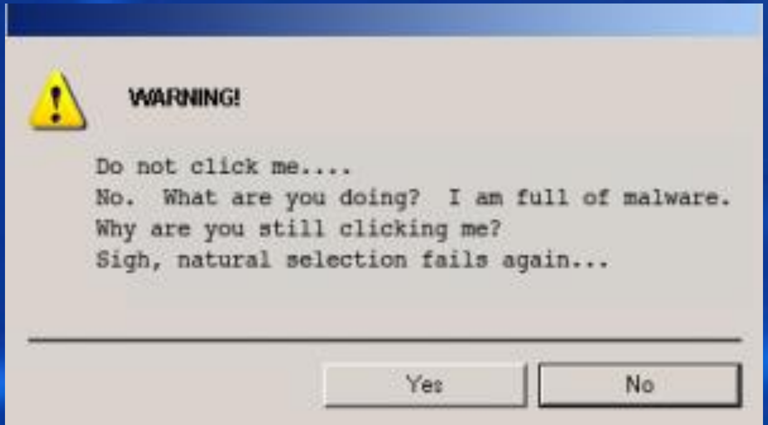


Project closed
master key for decrypt
440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software

we are sorry!

Securing the human

- Users are generally the weakest link in the chain.
- User education can reduce the incidence of malware in the enterprise
  - Recognizing suspicious emails or links
  - Be cautious of opening attachments or providing information over email
  - Promptly reporting incidents to the enterprise security team

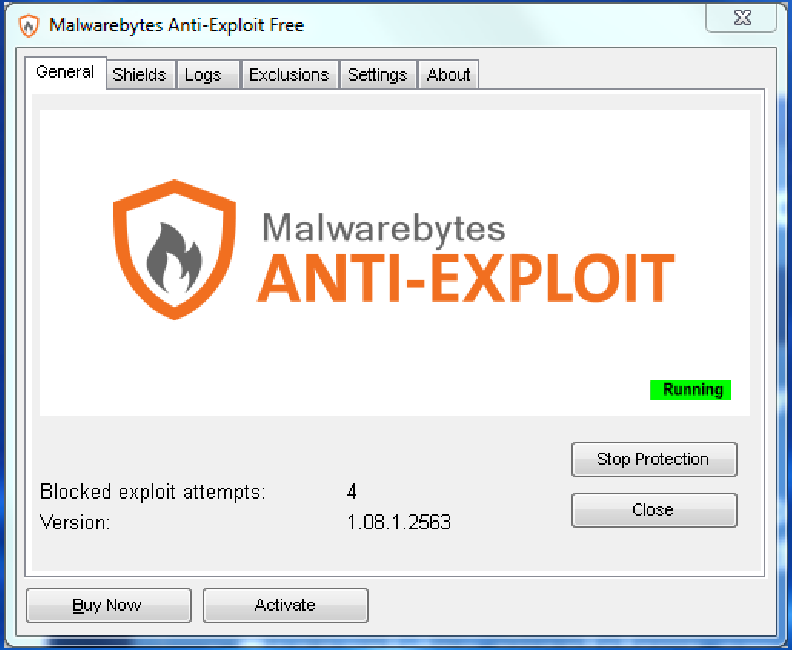


WARNING!

Do not click me....
No. What are you doing? I am full of malware.
Why are you still clicking me?
Sigh, natural selection fails again...

Securing the endpoint

- Limiting administrative access can improve odds of recovery via Volume Shadow Service (VSS).
- Group Policies can limit ransomware execution by targeting blocking executions in uncommon directories.
- Consider heuristics and specialized tools: Specialized anti-exploit and ransomware applications available (e.g. Malwarebytes Anti-Exploit / Anti-Ransomware)
- Endpoint agents such as Carbon Black or FireEye HX could provide insights to scope of ransomware infection and potentially block exploits on-the-fly.



Malwarebytes Anti-Exploit Free

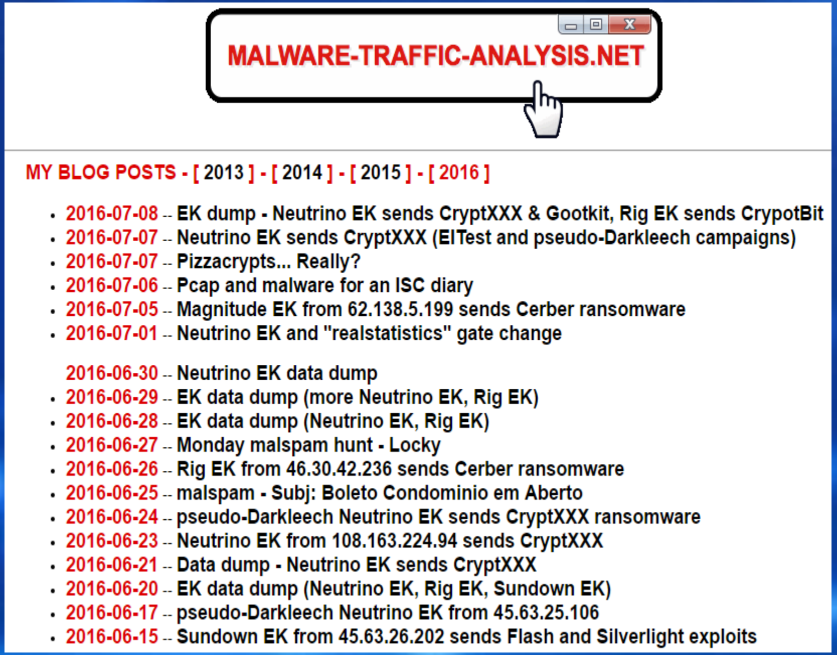
Blocked exploit attempts: 4
Version: 1.08.1.2563

Securing the network

- An up to date UTM / IP(D)S could provide some coverage for ransomware and exploit-kit attacks.
- Due to the polymorphic nature of many exploit kit vectors, not all vendors provide the same level of coverage (some vendors are not equipped to deal with these threats at all).
- Assume worst case scenarios – focus on detection as well as prevention.

Test, test, test…

- The best way to test your security defenses is by testing it against actual threats.
- Replaying traffic against IP(D)S systems can gauge effectiveness of protection.
  - ***Proofpoint Emerging Threats*** filters can be used to complement existing detection mechanisms.
- Malware blog sites can provide updates to the latest malware trends and/or actual samples for testing purposes.
  - ***Malware Traffic Analysis***
  - ***Malware Don’t Need Coffee***



MALWARE-TRAFFIC-ANALYSIS.NET

MY BLOG POSTS - [2013] - [2014] - [2015] - [2016]

- 2016-07-08 -- EK dump - Neutrino EK sends CryptXXX & Gootkit, Rig EK sends CrypotBit
- 2016-07-07 -- Neutrino EK sends CryptXXX (EITest and pseudo-Darkleech campaigns)
- 2016-07-07 -- Pizzacrypts... Really?
- 2016-07-06 -- Pcap and malware for an ISC diary
- 2016-07-05 -- Magnitude EK from 62.138.5.199 sends Cerber ransomware
- 2016-07-01 -- Neutrino EK and "realstatistics" gate change

2016-06-30 -- Neutrino EK data dump

- 2016-06-29 -- EK data dump (more Neutrino EK, Rig EK)
- 2016-06-28 -- EK data dump (Neutrino EK, Rig EK)
- 2016-06-27 -- Monday malspam hunt - Locky
- 2016-06-26 -- Rig EK from 46.30.42.236 sends Cerber ransomware
- 2016-06-25 -- malspam - Subj: Boleto Condominio em Aberto
- 2016-06-24 -- pseudo-Darkleech Neutrino EK sends CryptXXX ransomware
- 2016-06-23 -- Neutrino EK from 108.163.224.94 sends CryptXXX
- 2016-06-21 -- Data dump - Neutrino EK sends CryptXXX
- 2016-06-20 -- EK data dump (Neutrino EK, Rig EK, Sundown EK)
- 2016-06-17 -- pseudo-Darkleech Neutrino EK from 45.63.25.106
- 2016-06-15 -- Sundown EK from 45.63.26.202 sends Flash and Silverlight exploits

Securing the enterprise / infrastructure

- Know your systems! Have an inventory of all of your critical assets.
- Know your risks! Do you have a Business Impact Analysis (BIA) or a incident response (IR) plan in place?
- Frequent vulnerability assessments and/or penetration testing of the enterprise can reveal missing patches / vulnerabilities.
  - External scanning from the Internet provides a “hacker’s view” into the enterprise.
- Ensure all content management systems are fully up to date with latest security patches.

For more information

- Ransomware Hostage Rescue Manual
  - http://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf
- Department of Justice – Ransomware What It Is and What to Do About It
  - https://www.justice.gov/criminal-ccips/file/872766/download
- Malware Domain List
  - http://www.malwaredomainlist.com/mdl.php
- Suricata IP(D)S / Emerging Threats Ruleset
  - https://suricata-ids.org/
  - https://rules.emergingthreats.net/
- *Checkpoint: Inside Nuclear's Core*
  - http://blog.checkpoint.com/2016/04/20/inside-nuclears-core-analyzing-the-nuclear-exploit-kit-infrastructure/
- Malware Traffic Analysis
  - http://www.malware-traffic-analysis.net/blog-entries.html
- Malware Don't Need Coffee
  - http://malware.dontneedcoffee.com

Questions?